

Amendments to the Claims

1 Claim 1 (currently amended): A computer program product for efficiently generating pseudo-
2 random bits, the computer program product embodied on one or more computer readable media
3 and comprising:

4 computer-readable program code means for providing an input value comprising C
5 random bits;

6 computer-readable program code means for generating an output sequence [[of]]
7 comprising N pseudo-random bits using the provided C-bit input value as [[an]] a short exponent
8 x of a 1-way function $G^{**x} \bmod P$ that comprises comprising modular exponentiation modulo a
9 safe N-bit prime number P, wherein a length in bits, C, of the input value is substantially shorter
10 than a length in bits, N, of the generated output sequence and a base G of the modular
11 exponentiation is a fixed generator value;

12 computer-readable program code means for separating the N bits of the generated N-bit
13 output sequence into a C-bit portion and an (N-C)-bit portion; and

14 computer-readable program code means for using C selected bits the C-bit portion of the
15 generated N-bit output sequence as the provided input value for a next iteration of the computer-
16 readable program code means for generating while using all N-C remaining bits the (N-C)-bit
17 portion of the generated N-bit output sequence as pseudo-random output bits, until a desired
18 number of pseudo-random output bits have been generated.

1 Claim 2 (original): The computer program product according to Claim 1, wherein the 1-way
2 function is based upon an assumption known as "the discrete logarithm with short exponent"

Serial No. 09/753,727

-4-

RSW920000091US1

3 assumption.

Claims 3 - 5 (canceled)

1 Claim 6 (currently amended): The computer program product according to Claim 1, wherein C =
2 160 the length of the input value is ~~160~~ bits and N = 1024, a length of the safe prime number is
3 ~~1024~~ bits.

1 Claim 7 (currently amended): The computer program product according to Claim 1, wherein C is
2 greater than or equal to 160 and N is greater than or equal to 1024, the length of the input value is
3 ~~at least 160 bits and the length of the generated output sequence is at least 1024 bits.~~

Claim 8 (canceled)

1 Claim 9 (currently amended): The computer program product according to Claim 1, wherein the
2 (N-C)-bit portion is N - C remaining bits are concatenated to pseudo-random output bits
3 previously generated by the computer-readable program code means for generating.

1 Claim 10 (currently amended): The computer program product according to Claim 1, wherein
2 the (N-C)-bit portion is N - C remaining bits are selected from the N bits of the generated output
3 sequence as a contiguous group of (N-C) bits from the generated N-bit output sequence.

Serial No. 09/753,727

-5-

RSW920000091US1

1 Claim 11 (currently amended): The computer program product according to Claim 1, wherein
2 the (N-C)-bit portion is N-C remaining bits are selected from the N bits of the generated output
3 sequence as a non-contiguous group of (N-C) bits from the generated N-bit output sequence.

1 Claim 12 (previously presented): The computer program product according to Claim 1, further
2 comprising computer-readable program code means for using the desired number of generated
3 pseudo-random bits as input to an encryption operation.

1 Claim 13 (currently amended): A system for efficiently generating pseudo-random bits in a
2 computing environment, comprising:

3 means for providing an input value comprising C random bits;

4 means for generating an output sequence [[of]] comprising N pseudo-random bits using
5 the provided C-bit input value as [[an]] a short exponent x of a 1-way function $G^{**x} \bmod P$ that
6 comprises comprising modular exponentiation modulo a safe N-bit prime number P, wherein a
7 length in bits, C, of the input value is substantially shorter than a length in bits, N, of the
8 generated output sequence and a base G of the modular exponentiation is a fixed generator value;

9 means for separating the N bits of the generated N-bit output sequence into a C-bit
10 portion and an (N-C)-bit portion; and

11 means for using C selected bits the C-bit portion of the generated N-bit output sequence
12 as the provided input value for a next iteration of the means for generating while using all N-C
13 remaining bits the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random
14 output bits, until a desired number of pseudo-random output bits have been generated.

Serial No. 09/753,727

-6-

RSW920000091US1

1 Claim 14 (original): The system according to Claim 13, wherein the 1-way function is based
2 upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 15 - 17 (canceled)

1 Claim 18 (currently amended): The system according to Claim 13, wherein ~~the length of the~~
2 ~~input value is 160 bits~~ $C = 160$ and ~~a length of the safe prime number is 1024 bits~~ $N = 1024$.

1 Claim 19 (currently amended): The system according to Claim 13, wherein ~~the length of the~~
2 ~~input value C is at least 160 [[bits]] and the length of the generated output sequence N is at least~~
3 ~~1024 [[bits]].~~

Claim 20 (canceled)

1 Claim 21 (currently amended): The system according to Claim 13, wherein ~~the $N - C$ remaining~~
2 ~~bits are~~ $(N - C)$ -bit portion is concatenated to pseudo-random output bits previously generated by
3 the means for generating.

1 Claim 22 (currently amended): The system according to Claim 13, wherein ~~the $N - C$ remaining~~
2 ~~bits are selected from the N bits of the generated output sequence as~~ $(N - C)$ -bit portion is a
3 contiguous group of $(N - C)$ bits from the generated N -bit output sequence.

Serial No. 09/753,727

-7-

RSW920000091US1

1 Claim 23 (currently amended): The system according to Claim 13, wherein the ~~N-C~~ remaining
2 ~~bits are selected from the N bits of the generated output sequence as (N-C)-bit portion is a non-~~
3 ~~contiguous group of (N-C) bits from the generated N-bit output sequence.~~

1 Claim 24 (previously presented): The system according to Claim 13, further comprising means
2 for using the desired number of generated pseudo-random output bits as input to an encryption
3 operation.

1 Claim 25 (currently amended): A programmatic method for efficiently generating pseudo-
2 random bits, comprising the steps of:
3 providing an input value comprising C random bits;
4 generating an output sequence [[of]] comprising N pseudo-random bits using the
5 provided C-bit input value as [[an]] a short exponent x of a 1-way function $G^{**x} \bmod P$ that
6 comprises comprising modular exponentiation modulo a safe N-bit prime number P, wherein a
7 length in bits, C, of the input value is substantially shorter than a length in bits, N, of the
8 generated output sequence and a base G of the modular exponentiation is a fixed generator value;
9 separating the N bits of the generated N-bit output sequence into a C-bit portion and an
10 (N-C)-bit portion; and
11 using C-selected bits the C-bit portion of the generated N-bit output sequence as the
12 provided input value for a next iteration of the generating step while using all N-C remaining
13 bits the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random output bits,

Serial No. 09/753,727

-8-

RSW920000091US1

14 until a desired number of pseudo-random output bits have been generated.

1 Claim 26 (original): The method according to Claim 25, wherein the 1-way function is based
2 upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 27 - 29 (canceled)

1 Claim 30 (currently amended): The method according to Claim 25, wherein the length of the
2 input value is at least $C = 160$ [[bits]] and a length of the safe prime number is at least $N = 1024$
3 [[bits]].

Claim 31 (canceled)

1 Claim 32 (currently amended): The method according to Claim 25, wherein the length of the
2 input value is at least 160 bits and the length of the generated output sequence is at least 1024
3 bits C is greater than or equal to 160 and N is greater than or equal to 1024.

Claim 33 (canceled)

1 Claim 34 (currently amended): The method according to Claim 25, wherein the $N - C$ remaining
2 bits are $(N - C)$ -bit portion is concatenated to pseudo-random output bits previously generated by
3 the generating step.

Serial No. 09/753,727

-9-

RSW920000091US1

1 Claim 35 (currently amended): The method according to Claim 25, wherein the ~~N-C~~ remaining
2 bits are (N-C)-bit portion is selected from the N-bits of the generated output sequence as a
3 contiguous group of (N-C) bits from the generated N-bit output sequence.

1 Claim 36 (currently amended): The method according to Claim 25, wherein the ~~N-C~~ remaining
2 bits are (N-C)-bit portion is selected from the N-bits of the generated output sequence as a non-
3 contiguous group of (N-C) bits from the generated N-bit output sequence.

1 Claim 37 (previously presented): The method according to Claim 25, further comprising the step
2 of using the desired number of generated pseudo-random output bits as input to an encryption
3 operation.

Claim 38 (canceled)

1 Claim 39 (currently amended): An encryption system, comprising:
2 means for providing an input value comprising C random bits;
3 means for generating an output sequence [[of]] comprising N pseudo-random bits using
4 the provided C-bit input value as [[an]] a short exponent x of a 1-way function $G^{**x} \bmod P$ that
5 comprises comprising modular exponentiation modulo a safe N-bit prime number P , wherein a
6 length in bits, C , of the input value is substantially shorter than a length in bits, N , of the
7 generated output sequence and a base G of the modular exponentiation is a fixed generator value;

Serial No. 09/753,727

-10-

RSW920000091US1

8 means for separating the N bits of the generated N-bit output sequence into a C-bit
9 portion and an (N-C)-bit portion;

10 means for using ~~C selected bits~~ the C-bit portion of the generated N-bit output sequence
11 as the provided input value for a next iteration of the means for generating while using ~~all N-C~~
12 ~~remaining bits~~ the (N-C)-bit portion of the generated N-bit output sequence as pseudo-random
13 output bits, until a desired number of pseudo-random output bits have been generated; and

14 means for using the desired number of generated pseudo-random bits as input to an
15 encryption operation.

1 Claim 40 (original): The encryption system according to Claim 39, wherein the 1-way function
2 is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

Claims 41 - 43 (canceled)

1 Claim 44 (currently amended): The encryption system according to Claim 39, wherein ~~the length~~
2 ~~of the input value is 160 bits and a length of the safe prime number is 1024 bits~~ C = 160 and N =
3 1024.

Claims 45 - 46 (canceled)

1 Claim 47 (currently amended): The encryption system according to Claim 39, wherein ~~the N-C~~
2 ~~remaining bits are~~ (N-C)-bit portion is concatenated to pseudo-random output bits previously

Serial No. 09/753,727

-11-

RSW920000091US1

3 generated by the means for generating.

1 Claim 48 (new): The computer program product according to Claim 1, wherein N is greater than
2 or equal to $(C * 6)$.

1 Claim 49 (new): The system according to Claim 13, wherein N is greater than or equal to $(C * 6)$.
2

1 Claim 50 (new): The method according to Claim 25, wherein N is greater than or equal to $(C * 6)$.
2

1 Claim 51 (new): The encryption system according to Claim 39, wherein N is greater than or
2 equal to $(C * 6)$.

1 Claim 52 (new): A programmatic method for efficiently generating pseudo-random bits,
2 comprising the steps of:

3 providing an N-bit input value in which $(N-C)$ uppermost contiguous ones of the bits are
4 all set to zeroes and in which C lowermost contiguous ones of the bits are random;

5 generating an output sequence comprising N pseudo-random bits using the provided N-bit
6 input value as an effectively-short, C-bit exponent x of a 1-way function $G^{**}x \bmod P$ that
7 comprises modular exponentiation modulo a safe N-bit prime number P, wherein a base G of the
8 modular exponentiation is a fixed generator value;

Serial No. 09/753,727

-12-

RSW920000091US1

9 separating the N bits of the generated N-bit output sequence into a C-bit portion and an
10 (N-C)-bit portion;
11 creating a new N-bit input value in which the (N-C) uppermost contiguous ones of the
12 bits are all set to zeroes and in which the lowermost C contiguous ones of the bits are set to the
13 C-bit portion; and
14 using the new N-bit input value as the provided input value for a next iteration of the
15 generating step while using the (N-C)-bit portion of the generated N-bit output sequence as
16 pseudo-random output bits, until a desired number of pseudo-random output bits have been
17 generated.